Junos Pulse para Google Android

Guía del usuario

Versión
4.0

Junio de 2012
R1

Copyright © 2012, Juniper Networks, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen y ScreenOS son marcas comerciales registradas de Juniper Networks, Inc. en los Estados Unidos y otros países. El logotipo de Juniper, el logotipo de Junos y JunosE son marcas registradas de Juniper Networks, Inc. Todas las demás marcas comerciales, marcas de servicio, marcas comerciales registradas o marcas de servicio registradas pertenecen a sus respectivos propietarios. Juniper Networks no asume responsabilidad alguna por ningún error en el contenido del presente documento. Juniper Networks se reserva el derecho de cambiar, modificar, transferir o, de cualquier otra manera, modificar esta publicación sin previo aviso. Los productos fabricados o comercializados por Juniper Networks o sus componentes podrían estar incluidos en una o más de las siguientes patentes que posee en propiedad o mediante licencia a Juniper Networks: patentes de EE.UU. n.º 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186 y 6,590,785. Copyright © 2012, Juniper Networks, Inc. Todos los derechos reservados.

M3/9/12

Copyright © 2012, Juniper Networks, Inc.

Índice

Descarga e instalación de Junos Pulse 1
Funciones disponibles de Junos Pulse 1
Registro de seguridad 2
El panel de Mobile Security 3
Validación de dirección de correo electrónico 3
Utilización de las funciones de seguridad 3
Analizar/Amenazas detectadas 4
Backup (Respaldo) 6
Remote Monitoring (Supervisión remota) 7
Settings (Ajustes) 7
Ajustes de seguridad 8
Support Info (Información de asistencia) 8
Actualizar 9
Funciones antirrobo 9
Directivas de contraseñas y encriptación de información almacenada 11
Cancelar la señal acústica 11
Custom Button (Botón personalizado) 11
Desinstalación o borrado de datos 11
Adición de una conexión segura 12
Conexión 13
Visualización del icono de estado de la conexión 13
Visualización de la ventana de estado de conexión 13
Acceso limitado 13
Modos de interfaz de usuario 14
Problemas y limitaciones conocidos 14

Instalación y uso de Junos Pulse para Google Android

Junos Pulse le permite acceder a recursos de red protegidos desde su dispositivo Google Android™. También protege su dispositivo contra virus y malware, e incluye herramientas para reducir los riesgos inherentes en caso de pérdida o robo.

Puede encontrar información adicional para Junos Pulse, incluida información sobre las plataformas admitidas, en http://www.juniper.net/support/products/pulse/mobile/

Descarga e instalación de Junos Pulse

Utilice las instrucciones siguientes para descargar e instalar el software de Junos Pulse en los dispositivos con Google Android.

Nota informativa: El cliente Junos Pulse está disponible en la tienda de aplicaciones Google Play.

1. Desde el dispositivo con Android, descargue el software de Junos Pulse directamente al dispositivo. Una vez descargado, Junos Pulse se instala automáticamente.
2. Una vez que la aplicación se ha descargado e instalado, el icono de Junos Pulse aparecerá en el menú de aplicaciones.
3. La primera vez que inicie Junos Pulse, se mostrará el Acuerdo de Licencia de usuario final. Debe **Aceptar** la licencia para comenzar a usar Junos Pulse.

Funciones disponibles de Junos Pulse

Nota informativa: Junos Pulse se puede implementar con todas las funciones disponibles o con un subconjunto de ellas, según sus necesidades de uso. Es posible que su dispositivo no disponga de todas las funciones de Junos Pulse descritas aquí.

Junos Pulse puede incluir las funciones siguientes:

Ficha Seguridad

- **Analizar/Amenazas detectadas**: enumera las amenazas halladas en el dispositivo y da la opción de dar permiso o eliminar las aplicaciones sospechosas. Si no se encuentran amenazas, el botón muestra “Analizar”. Si se encuentran, el botón muestra Amenazas detectadas.
- **Backup** (Respaldo): permite hacer copia de seguridad de los Contactos y de los eventos del Calendario.
- **Remote Monitoring** (Supervisión remota): ofrece información sobre las actividades del dispositivo que están siendo supervisadas.
- **Anti Theft** (Antirrobo): enumera las funciones antirrobo activadas en el dispositivo.
- **Custom Button** (Botón personalizado): enlaza con una URL personalizada que abre una página web configurada por el proveedor de servicios.

Copyright © 2012, Juniper Networks, Inc.

Ficha VPN

Nota informativa: Este servicio solo se ofrece si se accede de forma segura a los recursos de la red corporativa.

- **Conexiones**: le permite agregar, editar y eliminar conexiones de red corporativas.
- **Intranet**: proporciona vínculos web configurados por su administrador.
- **Correo electrónico**: inicia la aplicación de correo electrónico.
- **Estado**: le permite ver, eliminar y enviar por correo electrónico los archivos de registro, lo que puede ser necesario para operaciones de solución de problemas. Los archivos de registro le muestran todos los incidentes de seguridad, como las horas de análisis para detección de virus y los virus descubiertos. Si cuenta con una conexión VPN establecida, también podrá ver el estado de dicha conexión en esta ventana.

Registro de seguridad

El conjunto Junos Pulse Mobile Security ofrece acceso a funciones que protegen su dispositivo frente a malware y virus, y le permite respaldar la información del calendario y los contactos en un servidor central. Deberá registrar su dispositivo antes de poder acceder a las funciones de seguridad.

Puede registrarse mediante un registro de URL automático o a través de un proceso de registro manual.

Registro automático mediante URL

Para realizar el registro automático mediante URL, tendrá que seleccionar una URL proporcionada por su administrador o proveedor de servicios. Cuando seleccione la URL, se le mostrará un mensaje para que verifique que dicha URL proviene de una fuente fiable. Al hacer clic en **Yes** (Sí) tras recibir este mensaje, tendrá lugar el proceso de registro de seguridad automático.

Para registrar las funciones de seguridad de forma automática, haga lo siguiente:

1. Inicie Junos Pulse.
2. Seleccione la URL de registro que le han proporcionado por correo electrónico, mensaje de texto o sitio web.
3. Debido a que el registro automático modifica los ajustes de seguridad de su dispositivo, deberá verificar la validez de la URL. Si está seguro de que la URL es fiable, seleccione **Yes** (Sí) cuando se le solicite.

Después de haber seleccionado Yes (Sí), el dispositivo estará registrado automáticamente para las funciones de seguridad.

Registro manual

En algunos casos, el registro manual también puede requerir que seleccione una URL. Cuando seleccione la URL, se le mostrará un mensaje para que verifique que dicha URL proviene de una fuente fiable. Al hacer clic en Yes (Sí) en la solicitud de registro, se mostrará la pantalla de registro manual.

La ventana de registro requiere la entrada de cierta información, como el código de licencia proporcionado por su administrador o proveedor de servicios.

Copyright © 2012, Juniper Networks, Inc.

Nota informativa: si utiliza un dispositivo con WIFI solamente (como una tableta sin servicio celular), el campo del número de teléfono no se mostrará en la ventana de registro.

Para registrar manualmente las funciones de seguridad, haga lo siguiente:

1. Inicie Junos Pulse.
2. Seleccione la **URL** que le han proporcionado por correo electrónico, mensaje de texto o sitio web.
3. Compruebe que la URL es fiable y haga clic en **Yes** (Sí) cuando se le solicite. Se abre la ventana de registro.
4. Escriba una dirección de **correo electrónico** y una **contraseña**.
5. Especifique el **código de licencia**.
6. El número de teléfono del dispositivo aparece en el cuadro **Número de teléfono**. Si el número no aparece, ingréselo manualmente, incluidos el código de país y el código de área sin los prefijos internacionales '00' ni '+'. No utilice espacios, paréntesis ni caracteres especiales. Los números de teléfono válidos tienen entre 11 y 15 dígitos (incluido el código de país).
7. Seleccione **Register** (Registrar).

El panel de Mobile Security

El panel es uno de los servidores con los que registra su dispositivo. Si obtiene acceso al panel (este acceso lo proporciona opcionalmente un administrador o el proveedor de servicios), puede iniciar sesión para supervisar su dispositivo, controlar ciertos parámetros de seguridad y cambiar su correo electrónico y su contraseña. Puede acceder a la interfaz web del panel a través de la URL que se le ha proporcionado. Para obtener información detallada sobre el inicio de sesión y los ajustes del panel, consulte la documentación del panel de Junos Pulse Mobile Security.

Validación de dirección de correo electrónico

Después de su primer inicio de sesión en el panel recibirá un mensaje de correo electrónico solicitándole que valide su dirección. Este mensaje incluye un enlace en el que deberá hacer clic a fin de validar su dirección de correo electrónico. Después de hacer clic en el enlace se abrirá una página web de notificación informando de que su dirección de correo electrónico ha sido validada.

Utilización de las funciones de seguridad

Después de registrarse correctamente, si su dispositivo utiliza Android 2.2 o superior, se abrirá la solicitud **Activate device administrator** (Activar administrador de dispositivo).

Nota informativa: Si no activa el administrador de dispositivo, algunas funciones se comportarán de forma distinta. Para obtener más detalles, consulte las secciones siguientes: “Funciones antirrobo” en la página 9 y “Desinstalación o borrado de datos” en la página 11.

Copyright © 2012, Juniper Networks, Inc.

Una vez registradas las funciones de seguridad, aparecerán las funciones disponibles, a las que podrá acceder desde la ficha Seguridad. Estas funciones son las siguientes:

- **Analizar/Amenazas detectadas**: enumera las amenazas (virus y malware) halladas en el dispositivo y da la opción de dar permiso o eliminar las aplicaciones sospechosas. Si no se encuentran amenazas, el botón muestra "Analizar". Si hace clic en él se abrirá la ventana "Analizar". Si se encuentran, el botón muestra Amenazas detectadas. Haga clic en él para ver las amenazas detectadas.

- **Backup** (Respaldo): permite hacer copia de seguridad de los Contactos y de los eventos del Calendario.
- **Remote Monitoring** (Supervisión remota): ofrece información sobre las actividades del dispositivo que están siendo supervisadas.
- **Settings** (Ajustes): disponible en la tecla Menu (Menú). Settings permite establecer intervalos de exploración, ver información de apoyo y registros de las aplicaciones, actualizar firmas de virus y actualizar el software Junos Pulse.

Analizar/Amenazas detectadas

El anti-virus y la detección de malware protegen su dispositivo al analizar todos los archivos y las tarjetas Secure Digital (SD) para impedir infecciones. Para ver las amenazas y configurar su detección:

1. Inicie Junos Pulse.
2. Seleccione la ficha **Seguridad**.
3. Si se han encontrado amenazas, haga clic en el botón **Amenazas detectadas**. Se abrirá la ventana Scan Results (Resultados del análisis).
4. En esta ventana se enumeran los virus, malware y aplicaciones sospechosas halladas en su dispositivo. Si su dispositivo no tiene la detección de amenazas habilitada, solo verá las aplicaciones prohibidas halladas en él.

Nota informativa: En caso de detectar una amenaza, en la barra de notificaciones aparecerá la notificación siguiente.

Ficha Detecciones

En la ficha Detecciones se muestran todos los elementos detectados. Puede seleccionar el botón naranja junto al elemento detectado para ver más información acerca de la detección y una lista de las acciones disponibles. Los tipos de detección y las acciones disponibles son:

- **Prohibited application** (Aplicación prohibida): se trata de una aplicación que se ha prohibido. Para eliminar una aplicación prohibida, seleccione el **botón naranja** junto al nombre de la aplicación y haga clic en el botón **Desinstalar**. Si no desinstala las aplicaciones prohibidas, el icono de notificación continuará apareciendo en la parte superior de la ventana de Junos Pulse.

Nota informativa: En algunos dispositivos, Junos Pulse puede desinstalar automáticamente aplicaciones que están prohibidas.

Copyright © 2012, Juniper Networks, Inc.

- **Malware crítico**: se trata de una aplicación instalada en su dispositivo que se sabe que es malware. Para eliminar malware, seleccione el **botón naranja** junto al nombre de la aplicación y haga clic en el botón **Desinstalar**. Si no desinstala las aplicaciones que tienen malware, el icono de notificación continuará apareciendo en la parte superior de la ventana de Junos Pulse.

Nota informativa: En algunos dispositivos, Junos Pulse puede desinstalar automáticamente aplicaciones que tienen malware.

- **Aplicación sospechosa**: se trata de una aplicación instalada en su dispositivo que tiene aspecto sospechoso. Una aplicación se considera sospechosa cuando la tecnología heurística ha determinado que la aplicación puede ser malware. En el caso de aplicaciones sospechosas, tiene la opción de dar permiso a la aplicación (agregarla a su Lista blanca) o desinstalarla. Para dar permiso a una aplicación sospechosa, seleccione el **botón naranja** junto al nombre de la aplicación y haga clic en el botón **Allow** (Permitir). Deberá también hacer clic en **Yes** (Sí) para confirmar la acción de Permitir, y luego hacer clic en **OK** (Aceptar) para confirmar que es consciente de que esta acción puede suponer un riesgo para su dispositivo (puede optar por ocultar el último cuadro de diálogo para que no vuelva a aparecer).

  Para desinstalar una aplicación sospechosa, seleccione el **botón naranja** junto al nombre de la aplicación y haga clic en el botón **Desinstalar**. Si no desinstala ni permite las aplicaciones sospechosas, el icono de notificación continuará apareciendo en la parte superior de la ventana de Junos Pulse.

  Haga clic en el botón **Ver detalles** para acceder a más información sobre las aplicaciones sospechosas. En la ventana de detalles también puede permitir o desinstalar la aplicación.

- **Virus**: los virus encontrados durante el último análisis se enumeran en la ficha Detecciones. Se recomienda eliminar los virus cuando aparecen aquí. Para eliminar el virus del dispositivo, seleccione el **botón naranja** junto al nombre del virus y haga clic en el botón **Eliminar**. Haga clic en el botón **Ver detalles** para acceder a más información sobre los virus detectados. También puede eliminar el virus desde la ventana de detalles.

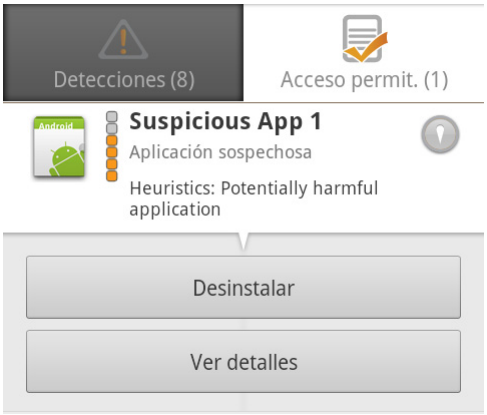
Copyright © 2012, Juniper Networks, Inc.

- **Botón Analizar**: el botón **Analizar** situado en la parte superior de la ficha **Detecciones** muestra cuánto tiempo hace del análisis más reciente del dispositivo. Puede hacer clic en el botón **Analizar** para abrir una ventana que le permite iniciar un análisis de dispositivo de uno de los tres tipos disponibles. Seleccione una de las opciones de análisis siguientes y haga clic en **OK** (Aceptar) para iniciar el análisis.
  - **Application scan** (Análisis de aplicaciones): analiza todas las aplicaciones no de sistema.
  - **Application and SD card scan** (Análisis de aplicaciones y tarjeta SD): analiza todas las aplicaciones no de sistema y la tarjeta SD.
  - **Full device scan** (Análisis total del dispositivo): analiza todos los archivos, aplicaciones que no son de sistema y la tarjeta SD.

Nota informativa: Al iniciar manualmente un análisis total del dispositivo, es posible que aparezca un aviso de uso de batería. Su propósito es informarle de que el análisis puede consumir una gran cantidad de batería. Por tanto, es conveniente tener el dispositivo cargándose durante el análisis.

Ficha Lista blanca

- Al dar permiso a una aplicación sospechosa detectada, la aplicación pasa a aparecer en la ficha Lista blanca. En la ficha Lista blanca puede gestionar las aplicaciones sospechosas si cambia de opinión y quiere desinstalar una aplicación permitida más adelante. Al seleccionar el **botón naranja** situado junto al nombre de la aplicación y hacer clic en el botón **Desinstalar** podrá desinstalar la aplicación incluida en la lista blanca. También puede hacer clic en el botón **Ver detalles** para ver más información sobre la aplicación, y desinstalarla desde la ventana de detalles.



Backup (Respaldo)

Junos Pulse Mobile Security respalda los contactos y la información de citas de calendario en una ubicación central. Para restaurar los datos, deberá ponerse en contacto con su administrador o acceder al panel. La restauración tendrá lugar en forma de un comando SMS que le indica a su dispositivo que debe contactar con el servidor para recuperar el respaldo.

Para respaldar los datos del dispositivo:

1. Inicie Junos Pulse.
2. Seleccione la ficha **Seguridad**.
3. Seleccione **Backup** (Respaldo). En el botón Backup (Respaldo) se muestra el momento del último respaldo.

Copyright © 2012, Juniper Networks, Inc.

4. En la ventana Backup (Respaldo) se muestra el número de Contactos y eventos de Calendario respaldados anteriormente. Para iniciar un respaldo, haga clic en el botón **Backup** (Respaldo) de la parte superior de la ventana. La copia de respaldo se iniciará inmediatamente.

Remote Monitoring (Supervisión remota)

En la ventana Remote Monitoring (Supervisión remota) podrá ver los tipos de eventos y las actividades del dispositivo que se están supervisando. Para ver la ventana Remote Monitoring (Supervisión remota), haga lo siguiente:

1. Inicie Junos Pulse.
2. Seleccione la ficha **Seguridad**.
3. Seleccione **Remote Monitoring** (Supervisión remota).

En la ventana Remote Monitoring (Supervisión remota) se pueden mostrar una o más de las actividades supervisadas siguientes:

Monitoring (Supervisión)

- SMS: se registran los mensajes SMS entrantes y salientes, lo que incluye el emisor, el receptor y el contenido de cada mensaje.
- MMS: actualmente no se admite el registro de mensajes MMS.
- Voice (Voz): se registran los eventos de historial de llamadas, como las llamadas salientes iniciadas y las llamadas entrantes recibidas (la duración de la llamada no se registra, pero sí el número de teléfono remoto).
- Log images/pictures (Registrar imágenes): si se activa la opción en el servidor, las imágenes descargadas o captadas en el dispositivo se convierten en miniaturas y se cargan en el servidor. Esta acción es inmediata y no depende de los límites de registro.

Registros:

- Event limit (Límite de eventos): cuando el número total de eventos (SMS, correo electrónico, voz) sobrepasa este límite, todos los registros se cargan en el servidor.
- File size limit (Límite de tamaño de archivo): cuando el tamaño combinado de los archivos de todos los registros (SMS, correo electrónico, voz) sobrepasa este límite, todos los registros se cargan en el servidor. Tenga en cuenta que los mensajes SMS suelen tener un tamaño de varios centenares de bytes. Los correos electrónicos suelen tener un tamaño de 2 KB o más (no se incluyen los adjuntos). Los mensajes de voz suelen tener un tamaño de unos 200 bytes.

Control:

- Periodic GPS updates (Actualizaciones periódicas de GPS): este período de actualización se configura en el servidor. Este parámetro consulta periódicamente la posición del dispositivo y carga la información en el servidor para seguimiento.
- Block calls (Bloquear llamadas): si está activado, bloquea todas las llamadas salientes.

Settings (Ajustes)

En la ventana Settings (Ajustes) se pueden configurar los parámetros de seguridad como las opciones de análisis y los intervalos de actualización de firmas de virus. También se puede ver información de asistencia y archivos de registro.

Copyright © 2012, Juniper Networks, Inc.

Desde la aplicación Junos Pulse se puede acceder a la ventana Settings (Ajustes) mediante el botón **Settings** (Ajustes). Para localizar el botón Settings (ajustes), haga lo siguiente:

- Seleccione los tres puntos verticales en el lado derecha de la barra **Action** (Acción) (en Android 4.0 o posterior) para acceder al menú. Seleccione **Settings** (Ajustes) en el menú.

- Seleccione el **botón Menu** (Menú) (Android 3.0 o anterior) para acceder al menú. Seleccione **Settings** (Ajustes) en el menú.

En la ventana Settings (Ajustes), puede acceder a las opciones siguientes:

Ajustes de seguridad

El administrador o el proveedor de servicios configuran los ajustes de seguridad y los cambios se descargan al dispositivo. Puede cambiar los ajustes de seguridad seleccionando la **flecha roja** junto a **Ajustes de seguridad** para acceder a lo siguiente:

- **Scan applications on install** (Analizar aplicaciones al instalarlas): si esta opción está activada, se inicia un análisis de la aplicación en el momento de instalarla. En los archivos descargados en /sdcard/download se lleva a cabo también un análisis de malware. Si la opción está desactivada, el análisis solo tiene lugar en el intervalo programado o si se inicia manualmente. Para activar esta opción, seleccione la casilla de verificación.
- **Scan SD Card on Insert** (Analizar tarjeta SD al insertarla): analiza la tarjeta SD en busca de malware y virus. Para activar esta opción, seleccione la casilla de verificación.
- **Scan inside archives** (Analizar dentro de archivos comprimidos): analiza el contenido de los archivos comprimidos, como .zip y .apk.
- **Optimize media scanning** (Optimizar análisis de archivos multimedia): permite analizar con mayor rapidez los archivos de fotos, música y multimedia, ya que no vuelve a analizar archivos grandes que ya se hayan analizado (a menos que se hayan modificado).
- **Full device scan** (Análisis total del dispositivo): muestra con qué intervalo de tiempo tiene lugar un análisis total del dispositivo. Un análisis total del dispositivo analiza todos los archivos, la tarjeta SD y las aplicaciones que no son de sistema. Para cambiar el intervalo de análisis utilice la flecha junto al intervalo de tiempo.
- **Profile update** (Actualización de perfil): en el momento de registrarse se cargan las definiciones de virus, que se actualizan según una programación preestablecida. Para cambiar el intervalo de actualización utilice la flecha junto al intervalo de tiempo.

Support Info (Información de asistencia)

Permite ver la información del dispositivo y de la aplicación Junos Pulse, así como ver y enviar registros seleccionando la **flecha naranja** junto a **Support Info** (Información de asistencia) en la ventana **Settings** (Ajustes). Esta acción abre la ventana Support Info (Información de asistencia), en la que puede hacer lo siguiente:

- Haga clic en el botón **View Logs** (Ver registros) para ver los datos del archivo de registro. Desde esta ventana de datos puede seleccionar el tipo de registro que desea ver en la lista desplegable, y también borrar el archivo de registro haciendo clic en el botón **Clear Logs** (Borrar registros).
- Haga clic en el botón **Send Logs** (Enviar registros) para seleccionar una aplicación desde la que enviar el archivo de registro.

Nota informativa: Los archivos de registro solo pueden enviarse desde una aplicación de correo electrónico. Actualmente no se admite ningún otro método.

Copyright © 2012, Juniper Networks, Inc.

Actualizar

La lista de virus y la aplicación Junos Pulse se pueden actualizar (si hay alguna actualización) seleccionando la **flecha naranja** junto a **Actualizar** en la ventana **Settings** (Ajustes). Esta acción abre la ventana Actualizar. En ella puede comprobar si hay actualizaciones para:

- **Virus List** (Lista de virus): si hay una actualización disponible, haga clic en el botón **Actualizar** para actualizar la lista de virus. Si no hay botón Actualizar, lo más probable es que la lista esté actualizada. Si hay un botón **Check** (Comprobar) disponible podrá comprobar si hay actualizaciones.
- **Application** (Aplicación): si hay una actualización disponible para Junos Pulse, haga clic en el botón **Actualizar** para actualizar su software. Si no hay botón Actualizar, lo más probable es que el software esté actualizado. Si hay un botón **Check** (Comprobar) disponible podrá comprobar si hay actualizaciones.

Funciones antirrobo

Existen una serie de medidas que puede tomar para proteger el dispositivo en caso de pérdida o robo. Si en su implementación de Junos Pulse estas funciones son visibles, en la pantalla de inicio de Junos Pulse aparecerá un botón **Anti Theft** (Antirrobo). Al hacer clic en este botón se enumeran las funciones antirrobo activadas en su dispositivo.

Puede hacer clic en el botón **Manage Anti-Theft Features** (Gestionar funciones antirrobo) de la ventana Anti Theft (Antirrobo) para abrir el sitio web de su proveedor de servicios a fin de adquirir o ver más funciones antirrobo.

Las funciones antirrobo incluyen:

- **Lock Handset** (Bloquear dispositivo) y **Unlock Handset** (Desbloquear dispositivo): bloquea el dispositivo hasta que se envíe un comando de desbloqueo desde el servidor o se introduzca una contraseña que se ajuste a la directiva de contraseñas del dispositivo. Cuando se envía un comando de bloqueo desde el servidor al dispositivo, también puede generarse una nueva contraseña. Esta contraseña se puede enviar por correo electrónico, y el usuario tiene la opción de modificarla. Cuando se activa el comando de bloqueo con esta contraseña que se acaba de generar, ocurre lo siguiente en diversos dispositivos:
  - Si el administrador del dispositivo está activado y el dispositivo ya tiene configurada una contraseña:
    - Cuando se envía un comando de bloqueo con una nueva contraseña, el dispositivo se bloquea con la contraseña existente. No se utiliza la nueva contraseña del servidor.
    - Cuando se envía un comando de bloqueo con una contraseña vacía, el dispositivo se bloquea con la contraseña existente. No se utiliza la contraseña del servidor.
  - Si el administrador del dispositivo está activado y el dispositivo no tiene configurada una contraseña:
    - Cuando se envía un comando de bloqueo con una nueva contraseña, el dispositivo se bloquea con esta nueva contraseña.
    - Cuando se envía un comando de bloqueo con una contraseña vacía, el dispositivo NO se bloquea.

Copyright © 2012, Juniper Networks, Inc.

- Si el administrador del dispositivo está desactivado y el dispositivo se registra automáticamente:
  - Cuando se envía un comando de bloqueo con una nueva contraseña, el dispositivo se bloquea con esta nueva contraseña. (Independientemente de la contraseña configurada en el dispositivo).
  - Cuando se envía un comando de bloqueo con una contraseña vacía, el dispositivo NO se bloquea.
- Si el administrador del dispositivo está desactivado y el dispositivo se registra manualmente:
  - Cuando se envía un comando de bloqueo con una nueva contraseña, el dispositivo se bloquea con esta nueva contraseña. (Independientemente de la contraseña configurada en el dispositivo).
  - Cuando se envía un comando de bloqueo con una contraseña vacía, el dispositivo NO se bloquea.

- Botón de **llamada de emergencia**: cuando el dispositivo está bloqueado, existe un botón de llamada de emergencia disponible en la ventana de desbloqueo. Esto le permite realizar una llamada a un número de emergencia, por ejemplo, cuando seleccione este botón y marque dicho número.
- **SIM Change** (Cambio de SIM) (en Android 2.2 y superior): si la función de administrador del dispositivo está activada y se activa la función Wipe (Borrar), un comando de limpieza restablece el dispositivo a los ajustes originales de fábrica. No se lleva a cabo bloqueo alguno. Si la función de administrador del dispositivo no está activada y se cambia la tarjeta SIM, el dispositivo activa el modo GPS por robo y se bloquea.
- **SIM Change** (Cambio de SIM) (en Android OS 2.1): el dispositivo cambia a modo GPS por robo y se bloquea. Si la función Wipe (Borrar) está activada, la información sensible se borra automáticamente del dispositivo.
- **Wipe Handset** (Borrar dispositivo) (en Android OS 2.2 y superior): si la función de administrador del dispositivo está activada, un comando de limpieza enviado desde el servidor restablece el dispositivo a los ajustes originales de fábrica. Si la función de administrador del dispositivo no está activada, un comando de limpieza elimina la información de programación, contactos y tareas, los mensajes SMS y el contenido de la tarjeta de memoria.
- **Wipe Handset** (Borrar dispositivo) (en Android OS 2.1): elimina la información de programación, contactos y tareas.
- **Send Backup** (Enviar respaldo): si estos datos no están almacenados en el servidor, esta función recopila la información de respaldo del dispositivo y la envía por correo electrónico a la dirección de correo electrónico proporcionada en el proceso de registro.
- **GPS Location** (Ubicación por GPS): si el dispositivo está equipado con GPS, el administrador podrá ubicarlo. La ubicación del dispositivo se muestra en el servidor de Junos Pulse.
- **Alarm On and Off** (Activación/desactivación de alarma) (Scream locate; Localización acústica): emite un sonido de alarma con un volumen máximo para ubicar el dispositivo cuando se encuentra en un lugar cercano.
- **GPS Theft On and Off** (Activación/desactivación de GPS por robo): envía actualizaciones del GPS al servidor de Junos Pulse cada 2 a 5 minutos para ajustar la ubicación por GPS en caso de robo del dispositivo.

Copyright © 2012, Juniper Networks, Inc.

Directivas de contraseñas y encriptación de información almacenada

Junos Pulse puede forzar la aplicación de directivas de contraseñas y de encriptación de información en su dispositivo. Esto significa que será obligatorio utilizar una contraseña de dispositivo y establecer una encriptación de los datos del dispositivo que cumpla los criterios de la directiva de seguridad de Junos Pulse.

Una directiva de contraseñas puede incluir, pero no se limita a, requisitos como el número de caracteres exigidos, la frecuencia con la que se debe modificar la contraseña, el número de intentos fallidos de introducción de la contraseña antes de que se borren completamente los datos del dispositivo y el tiempo que el dispositivo puede permanecer inactivo antes de que tenga lugar un bloqueo automático. Asimismo, la contraseña se puede restablecer a distancia y enviar por correo electrónico. Por ejemplo, si se dispositivo se bloquea a distancia, un comando de desbloqueo puede restablecer la contraseña con la nueva contraseña enviada por correo electrónico.

Si no ha configurado una contraseña de dispositivo o si la contraseña no cumple los requisitos de la directiva de contraseñas, se le solicitará que restablezca la contraseña para que cumpla esos requisitos.

Como parte de la directiva de seguridad del dispositivo, quizá se le solicite la encriptación de sus datos de aplicaciones. En tal caso, una solicitud le informará de este requisito. La solicitud se repetirá continuamente hasta que active la función de encriptación de datos en su dispositivo. Si, pasado un tiempo, no ha cumplido los requisitos de la directiva de seguridad, es posible que el dispositivo sea bloqueado o limpiado a distancia.

Cancelar la señal acústica

Desde el panel se puede enviar un comando acústico al dispositivo que le permitirá encontrar el dispositivo de forma sonora si se encuentra a una distancia audible, incluso con los altavoces y el timbre silenciados. Una vez ubicado el dispositivo, puede apagar la señal acústica desde la barra de **notificación**. Seleccione la notificación **Scream activated** (Señal acústica activada) para cancelar esta señal.

Custom Button (Botón personalizado)

Si su implementación de Junos Pulse muestra esta función, en su pantalla de inicio aparecerá un botón adicional, personalizado por su proveedor de servicios. Al hacer clic en este botón, una URL personalizada abrirá la página web configurada por el proveedor de servicios. Esa página puede ofrecer la compra de funciones adicionales, o quizá mostrar información adicional, dependiendo del proveedor de servicios.

Desinstalación o borrado de datos

Quizá deba volver a registrar su dispositivo tras el registro inicial o puede que necesite borrar los ajustes de Junos Pulse del dispositivo por alguna razón. Puede conseguir esto desinstalando Junos Pulse o borrando manualmente todos los ajustes del siguiente modo.

1. Desde el menú principal, seleccione **Settings** > (Ajustes)> **Applications** (Aplicaciones) > **Manage Applications** (Administrar aplicaciones) > Junos Pulse.
2. Para desinstalar Junos Pulse, seleccione el botón **Desinstalar**.

O bien:

3. Para borrar todos los datos de Junos Pulse, seleccione el botón **Clear data** (Borrar datos).

Copyright © 2012, Juniper Networks, Inc.

Si la función de **administrador del dispositivo** está activada, puede desinstalar Junos Pulse haciendo lo siguiente:

1. En el menú principal, seleccione **Settings** (Ajustes)> **Location & Security** (Ubicación y seguridad) (en algunos dispositivos es solo **Seguridad**).
2. Seleccione **Device Administrator** (Administrador del dispositivo) y deseleccione la casilla de verificación **Junos Pulse**. Ahora puede iniciar el proceso normal de desinstalación.

Adición de una conexión segura

Nota informativa: Este servicio solo se ofrece si se accede de forma segura a los recursos de la red corporativa.

Junos Pulse usa la conectividad 3G, 4G, Edge o WIFI de su dispositivo para establecer una conexión autenticada con una red protegida. Puede agregar una conexión para cada red diferente a la que se conecte. Se trata de una conexión VPN segura a su red corporativa, o un canal SSL de acceso central a los marcadores web configurados por su administrador.

Para definir una conexión, realice lo siguiente:

1. Inicie Junos Pulse.
2. En la ficha **VPN**, seleccione **Conexiones**.
3. Seleccione **Add Connection** (Agregar conexión).
4. Introduzca las siguientes propiedades de conexión:
   - **Connection name** (Nombre de la conexión): un nombre descriptivo.
   - **URL:** la dirección web proporcionada por el administrador de red.

   (Observe que el nombre y la URL de la conexión son los únicos campos obligatorios para crear un perfil de conexión. El resto de campos son opcionales.)
   - **Username** (Nombre de usuario): introduzca su nombre de usuario.
   - **Territorio**: si su administrador le ha proporcionado esta información, introduzca el territorio.
   - **Rol**: si su administrador le ha proporcionado esta información, introduzca el rol.
   - **Uses Certificate** (Usa certificado): seleccione esta casilla de verificación si su administrador le ha proporcionado un certificado digital. Si no usa un certificado, debe proporcionar un nombre de usuario y contraseña al conectarse.
   - **Certificate Path** (Ruta de certificado): esta casilla está disponible si seleccionó la casilla de verificación Usa certificado. Seleccione **Pick** (Elegir) para buscar el archivo de certificado. (Observe que este campo es obligatorio si ha seleccionado Uses Certificate [Usa certificado].)
   - **Key Path** (Ruta de clave): esta casilla está disponible si seleccionó la casilla de verificación Usa certificado. Seleccione **Pick** (Elegir) para buscar la clave de red que le proporcionó su administrador. (Observe que este campo es obligatorio si ha seleccionado Uses Certificate [Usa certificado].)
5. Seleccione **Create Connection** (Crear conexión). Ahora se habrá creado y guardado su conexión.

Copyright © 2012, Juniper Networks, Inc.

Conexión

Una vez configurada su conexión, seleccione el botón **Conectar**.

Si el campo **Select Connection** (Seleccionar conexión) no muestra la conexión predeterminada correcta, puede seleccionarla en el menú desplegable. Quizá deba ingresar información adicional que necesitará la red cuando establezca una conexión.

Visualización del icono de estado de la conexión

El estado de su conexión actual se muestra también en la parte inferior de la ventana de Junos Pulse como un icono. El aspecto del icono indica si la conexión está activa, inactiva o limitada por incumplimiento de la normativa (consulte Acceso limitado en la página 13).

Conexión activa Sin sesión Acceso limitado

El icono de conexión activa aparece también en la barra de estado de la parte superior de la ventana del dispositivo. Al cerrar Junos Pulse, este icono permanece visible siempre que su conexión VPN esté activa.

Visualización de la ventana de estado de conexión

Si tiene una conexión VPN completa establecida (no todos los dispositivos admiten conexión VPN completa), al seleccionar el botón **Estado** de la ventana principal se muestra la siguiente información de VPN:

- VPN Status (Estado de VPN): Connected (Conectada) o Disconnected (Desconectada)
- Server (Servidor): URL del servidor
- Duración
- Bytes enviados
- Bytes recibidos
- Address (Dirección)

En la barra de notificación, se mostrará también la notificación siguiente cuando tenga una conexión VPN activa.

Nota informativa: Si solo tiene acceso a los marcadores web (Acceso central en lugar de Acceso VPN), el estado de VPN es “Disconnected” (Desconectada), pero el icono de conexión de Junos Pulse aparecerá en la parte inferior de la ventana de Junos Pulse.

Acceso limitado

Para garantizar la integridad de los dispositivos móviles que acceden a recursos de red, un administrador puede imponer una directiva de seguridad que los dispositivos móviles deben cumplir para poder conectarse a la red. Si se detecta que un dispositivo móvil no la cumple al intentar acceder a una conexión de red segura, es posible que solo se conceda un acceso limitado. Si su dispositivo no cumple la normativa, se le mostrará esta información y quizá un botón **Continuar** en el que puede hacer clic para obtener acceso de red limitado.

Estas son algunas de las posibles razones para el incumplimiento de la normativa:

- Su dispositivo se ha manipulado para darle acceso “root (raíz)”.
- Su dispositivo ejecuta un sistema operativo no permitido por la normativa de seguridad.
- Su dispositivo no está registrado y activo con la Mobile Security Gateway (MSG) apropiada, o Junos Pulse Mobile Security Suite no está activo en el dispositivo.

Deberá solucionar el problema de incumplimiento antes de poder establecer una conexión de red completa.

Copyright © 2012, Juniper Networks, Inc.

Modos de interfaz de usuario

Su administrador o proveedor de servicios puede implementar Junos Pulse en su dispositivo con diversos conjuntos de funciones, disponibles a través de la interfaz de usuario de Junos Pulse. Puede utilizar una interfaz de usuario completa, con todas las funciones posibles de Junos Pulse a la vista, o una interfaz de usuario mínima o de seguridad que incluye un subconjunto de funciones de Junos Pulse visibles. Los posibles modos de interfaz de usuario que el administrador puede implementar en su dispositivo son:

- **Full UI** (Interfaz de usuario completa): incluye todas las funciones de Junos Pulse disponibles, según se describe en este manual.
- **Minimal UI** (Interfaz de usuario mínima): incluye la pantalla de bienvenida de Junos Pulse, el Acuerdo de licencia de usuario final y una pantalla de inicio con un menú Acerca de. Solo en los dispositivos compatibles, los virus, malware y aplicaciones prohibidas detectados se eliminan automáticamente. En el caso de malware y aplicaciones prohibidas, se muestra una notificación al eliminar una aplicación. Al hacer clic en la notificación se abre una pantalla con información sobre la aplicación eliminada. Haga clic en el botón **Clear** (Borrar) para cerrar la notificación.
- **Security UI** (Interfaz de usuario de seguridad): esta interfaz de usuario solo incluye las funciones de seguridad de Junos Pulse y no ofrece la capacidad de efectuar conexiones VPN.

Problemas y limitaciones conocidos

- Android tiene limitaciones de compatibilidad con certificados. Si experimenta un error “No cert”, o si Junos Pulse se cierra inesperadamente al intentar conectar, póngase en contacto con el administrador.
- En este momento, solo es posible enviar archivos de registro por correo electrónico. No se admite ningún otro método.
- Aunque Photo and Video Share (Compartir fotos y vídeos) aparece como opción al seleccionar Send Logs (Enviar registros), no es un método de envío de registros válido. No seleccione esta opción al enviar archivos de registro.
- Cuando el dispositivo está bloqueado, ya sea por el comando Handset Lock (Bloquear dispositivo) o por el comando Lock on SIM Change (Bloquear al cambiar SIM), quizá aún pueda acceder a la ventana de inicio y a la de notificaciones.
- Si un dispositivo no tiene acceso a servicio de red móvil, no puede recibir comandos. Por ejemplo, si un dispositivo solo está conectado a WiFi, no puede recibir comandos como Lock (Bloquear) o Wipe (Borrar).
- Si la función de administrador del dispositivo no está activada, la función de eliminación automática de malware y aplicaciones prohibidas, así como la eliminación automática de aplicaciones, solo están disponibles en determinados dispositivos Samsung. Para obtener información más detallada, consulte la Junos Pulse Supported Platforms Guide (Guía de plataformas compatibles).
- Si su dispositivo se registra con el MSG mediante registro automático, la función Lock on SIM Change (Bloquear al cambiar SIM) está activada y cambia la SIM, la única forma de desbloquear el dispositivo es poner de nuevo la SIM original y enviar un comando de desbloqueo al dispositivo desde el panel.

Copyright © 2012, Juniper Networks, Inc.

Índice

A

acceso limitado, incumplimiento . . . 13
actualizar . . . 9
acuerdo de licencia de usuario final . . . 1
administrador del dispositivo . . . 3
ajustes . . . 7
ajustes de seguridad . . . 8
amenazas detectadas . . . 4
analizar dentro de archivos comprimidos . . . 8
Analizar, botón . . . 6
antirrobo, funciones . . . 9
  activación y desactivación de alarma, localización acústica . . . 10
  bloquear dispositivo, establecer nueva contraseña . . . 9
  botón de llamada de emergencia . . . 10
  cambio de SIM . . . 10
  desbloquear dispositivo, establecer nueva contraseña . . . 9
  enviar respaldo . . . 10
  GPS por robo . . . 10
  ubicación por GPS . . . 10
antivirus . . . 4
aplicaciones prohibidas . . . 4

B

borrar datos . . . 11

C

código de licencia . . . 3
conexión . . . 12, 13
  agregar una conexión . . . 12
  certificado . . . 12
  clave . . . 12
  icono de estado . . . 13
  nombre de usuario . . . 12
  pantalla de estado, VPN completa . . . 13
  rol . . . 12
  territorio . . . 12
  URL . . . 12
conexión segura . . . 13

D

descargar aplicación . . . 1
desinstalar . . . 11
Detecciones, ficha . . . 4
dirección de correo electrónico, validación . . . 3
directiva de contraseñas . . . 11
dispositivos con WIFI solamente . . . 3

E

eliminación automática de aplicaciones . . . 4
emergencia, botón de llamada de . . . 10
encriptación de información almacenada . . . 11
enviar registros . . . 8

F

funciones de seguridad . . . 2
  antivirus, detección de malware . . . 4
  registrar para . . . 2
  registro automático de URL . . . 2
  registro manual . . . 2
funciones disponibles . . . 1

I

información de asistencia . . . 8
instalación . . . 1

M

malware, aplicaciones . . . 5
Mobile Security, panel . . . 3
modos de interfaz de usuario . . . 14

O

optimizar el análisis de archivos multimedia . . . 8

P

panel . . . 3
perfil, actualizar . . . 8
personalizado, botón . . . 11

R

registro automático de URL . . . 2
registro manual . . . 2
respaldo de datos . . . 6
resultados de análisis
  aplicaciones prohibidas . . . 4
  malware . . . 5
  prohibidas . . . 4
  sospechosas . . . 5
  virus . . . 5

S

señal acústica, cancelación . . . 11
sospechosas, aplicaciones . . . 5
supervisión remota . . . 7

Copyright © 2012, Juniper Networks, Inc.

V

validar dirección de correo electrónico 3
ver registros 8
virus 5

Copyright © 2012, Juniper Networks, Inc.